IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of:	Group Art Unit: 2136
Joshua D. Hug	Confirmation No. 1315
Application No.: 10/719,674	Examiner: Johnson, Carlton
Filed: November 21, 2003	
For: RIGHTS ENFORCEMENT AND USAGE REPORTING ON A CLIENT DEVICE	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

TO THE COMMISSIONER FOR PATENTS:

In response to the Advisory Action dated August 9, 2007 ("Advisory Action"), and the Office Action dated June 7, 2007 ("Final Office Action"), Applicant requests review of the final rejection in the above-identified application.

Listing of the Claims begins on page 2 of this paper.
Remarks/Arguments begin on page 12 of this paper.

Listing of Claims:

1. (Previously Presented) A method comprising:
   obtaining an integrity hash of rights information stored in a clear form at a client device, said rights information being associated with content stored at the client device;
   encrypting the integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device; and
   storing the encrypted hash on the client device.

2. (Original) The method of claim 1 wherein obtaining the integrity hash comprises:
   receiving the integrity hash from a server device.

3. (Original) The method of claim 1 wherein obtaining the integrity hash comprises:
   generating the integrity hash on the client device.

4. (Original) The method of claim 3 wherein generating the integrity hash on the client device comprises:
   applying the client device key in a combination with the rights information; and
   determining the integrity hash from the combination of the rights information and the client device key.

5. (Original) The method of claim 1 wherein the integrity hash comprises a first integrity hash, the method further comprising:
   obtaining a second integrity hash of the rights information; and
   storing the second integrity hash on the client device in a clear form.

6. (Original) The method of claim 5 wherein obtaining the second integrity hash comprises:
   receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

7. (Original) The method of claim 5 wherein obtaining the first integrity hash comprises:

applying the client device key in a combination with the rights information and the second integrity hash; and

determining the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

8. (Original) The method of claim 1 further comprising:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

9. (Original) The method of claim 1 further comprising:

generating a validation hash from at least the rights information;

decrypting the encrypted hash to recover the integrity hash; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

10. (Original) The method of claim 9 further comprising:

disabling the content on the client device if tampering is detected.

11. (Original) The method of claim 1 further comprising:

storing the rights information on the client device in a clear form.

12. (Original) The method of claim 10 further comprising:

reading the rights information from the client device in the clear form out to a server device.

13. (Original) The method of claim 1 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content;

updating the rights information with changes in usage;

regenerating, re-encrypting, and restoring the integrity hash on the client device for each update of the rights information.

14. (Original) The method of claim 1 wherein the integrity hash comprises a Hash Message Authentication Code (HMAC).

15. (Original) The method of claim 1 wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path.

16. (Original) The method of claim 1 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

17. (Original) The method of claim 1 further comprising at least one of:
downloading the rights information from a server device; and
installing a storage medium having the rights information stored thereon.

18. (Original) The method of claim 1 wherein the rights information grant unlimited play for the content on the client device.

19. (Original) The method of claim 3 wherein generating the integrity hash comprises generating the integrity hash in trusted hardware.

20. (Original) A method comprising:
obtaining a first integrity hash of rights information stored at a client device, said rights information being associated with content stored at the client device, said first integrity hash having been generated using an external key as an integrity secret;
obtaining a second integrity hash of the rights information;
encrypting the second integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device;
storing the rights information and the first integrity hash at the client device in a clear form; and
storing the encrypted hash at the client device.

21. (Original) The method of claim 20 further comprising:
receiving a content key at the client device for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

22. (Original) The method of claim 20 wherein obtaining the first integrity hash comprises:

receiving the external key at the client device; and

generating the first integrity hash at the client device using the external key.

23. (Original) The method of claim 20 wherein obtaining the first integrity hash comprises:

receiving the first integrity hash from a server device.

24. (Original) The method of claim 20 wherein obtaining the second integrity hash comprises:

receiving the second integrity hash from a server device; and

receiving a key used by the server device to generate the second integrity hash.

25. (Original) The method of claim 20 wherein obtaining the second integrity hash comprises:

generating the second integrity hash at the client device using the client device key as an integrity secret.

26. (Original) The method of claim 20 further comprising:

reading the rights information and the first integrity hash from the client device in the clear form out to a server device;

generating a validation hash, using the external key, of at least the rights information read from the client device; and

comparing the validation hash to the first integrity hash to detect tampering.

27. (Original) The method of claim 20 further comprising:

generating a validation hash from at least the rights information;

decrypting the encrypted hash using the client device key to recover the second integrity hash; and

comparing the validation hash to the second integrity hash to detect tampering.

28. (Original) The method of claim 20 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content; and

updating the rights information with changes in usage.

29. (Original) The method of claim 28 further comprising:

regenerating and restoring the first integrity hash on the client device for each update.

30. (Original) The method of claim 28 further comprising:

regenerating, re-encrypting, and restoring the second integrity hash on the client device for each update.

31. (Previously Presented) A method comprising:

generating a validation hash from at least stored clear form rights information associated with content stored on a client device;

decrypting an encrypted hash to recover an integrity hash using a client device key that is externally inaccessible from the client device, said integrity hash having been previously generated from at least the stored clear form rights information associated with the content; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

32. (Original) The method of claim 31 further comprising:

disabling the content on the client device if tampering is detected.

33. (Original) The method of claim 31 further comprising:

receiving a usage request for the content stored at the client device, said usage request to initiate generation of the validation hash and comparison to the integrity hash; and

permitting usage only if the content is not disabled.

34. (Previously Presented) A client device comprising:

a register to store a client device key, said register being externally inaccessible from the client device;

a memory to store content and clear form rights information associated with the content, said memory being externally accessible;

hash circuitry to obtain an integrity hash of the rights information; and

encryption circuitry to encrypt the integrity hash using the client device key to generate an encrypted hash;

said memory to store the encrypted hash.

35. (Original) The client device of claim 34 wherein the hash circuitry is to obtain the integrity hash from a server device.

36. (Original) The client device of claim 34 wherein the hash circuitry is to generate the integrity hash on the client device.

37. (Original) The client device of claim 36 wherein, to generate the integrity hash, the hash circuitry is to apply the client device key in a combination with the rights information, and to determine the integrity hash from the combination of the rights information and the client device key.

38. (Original) The client device of claim 34 wherein the integrity hash comprises a first integrity hash, the hash circuitry further to obtain a second integrity hash of the rights information, said memory to store the second integrity hash in a clear form.

39. (Original) The client device of claim 38 wherein, to obtain the second integrity hash, the hash circuitry is to receive the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

40. (Original) The client device of claim 38 wherein, to obtain the first integrity hash, the hash circuitry is to apply the client device key in a combination with the rights information and the second integrity hash, and to determine the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

41. (Original) The client device of claim 34 wherein the encryption circuitry is to encrypt a content key for the content using the client device key to generate an encrypted content key; and

the memory is to store the encrypted content key on the client device.

42. (Original) The client device of claim 34 wherein the hash circuitry is to generate a validation hash from at least the rights information; and

the encryption circuitry is to decrypt the encrypted hash to recover the integrity hash;

the client device further comprising:

a comparator to compare the validation hash to the integrity hash to detect tampering with the rights information.

43. (Original) The client device of claim 42 further comprising:

a content controller to disable the content on the client device if tampering is detected.

44. (Previously Presented) The client device of claim 34 wherein the memory is to store the rights information in a clear form along with an encrypted hash.

45. (Original) The client device of claim 34 wherein the rights information comprise usage information, the client device further comprising:

tracking circuitry to track usage of the content and update the rights information changes in usage;

wherein the hash circuitry and the encryption circuitry are to regenerate, re-encrypt, and restore the integrity hash in the memory for each update of the rights information.

46. (Original) The client device of claim 34 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

47. (Original) The client device of claim 34 further comprising at least one of:

an input port to download the rights information from a server device; and

a storage medium port to receive a storage medium having the rights information stored thereon.

48. (Original) The client device of claim 47 wherein the memory at least partially comprises the storage medium.

49. (Previously Presented) A machine readable medium having stored thereon machine executable instructions, the execution of which to implement a method comprising:

receiving clear form rights information at a client device, said rights information being associated with content stored on the client device, said client device having a client device key that is externally inaccessible from the client device;

storing the rights information on the client device in a clear form;

obtaining an integrity hash of the rights information;

encrypting the integrity hash using the client device key to generate an encrypted hash; and

storing the encrypted hash on the client device.

50. (Original) The machine readable medium of claim 49 wherein obtaining the integrity hash comprises:

receiving the integrity hash from a server device.

51. (Original) The machine readable medium of claim 49 wherein obtaining the integrity hash comprises: generating the integrity hash on the client device.

52. (Original) The machine readable medium of claim 49 wherein generating the integrity hash on the client device comprises:

applying the client device key in a combination with the rights information; and

determining the integrity hash from the combination of the rights information and the client device key.

53. (Original) The machine readable medium of claim 49 wherein the integrity hash comprises a first integrity hash, the method further comprising:

obtaining a second integrity hash of the rights information; and

storing the second integrity hash on the client device in a clear form.

54. (Original) The machine readable medium of claim 53 wherein obtaining the second integrity hash comprises:

receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

55. (Original) The machine readable medium of claim 53 wherein obtaining the first integrity hash comprises:

applying the client device key in a combination with the rights information and the second integrity hash; and

determining the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

56. (Original) The machine readable medium of claim 49 wherein the method further comprises:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

57. (Original) The machine readable medium of claim 49 wherein the method further comprises:

generating a validation hash from at least the rights information;

decrypting the encrypted hash to recover the integrity hash; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

58. (Original) The machine readable medium of claim 57 wherein the method further comprises:

disabling the content on the client device if tampering is detected.

59. (Previously Presented) The machine readable medium of claim 49 wherein the rights information grants unlimited play for the content on the client device.

60. (Original) The machine readable medium of claim 59 wherein the method further comprises:

reading the rights information from the client device in the clear form out to a server device.

61. (Original) The machine readable medium of claim 49 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content;

updating the rights information with changes in usage;

regenerating, re-encrypting, and restoring the integrity hash on the client device for each update of the rights information.

REMARKS/ARGUMENTS

35 U.S.C. §102 Rejections

Applicants respectfully submit that the §102 rejections in the Office Action are clearly improper and without basis. This clear error lead the Examiner to incorrectly conclude that the present application is anticipated by Published U.S. Patent application No. 2003/0046238 to Nonaka et al. (hereinafter "*Nonaka*").

Independent Claims 1, 20, 31, 34, and 49 were previously amended to clarify that "the present invention can store rights and/or usage information **in clear form** on a client device while still providing security for the content and integrity for the rights/usage information." *See* the published version of the current application (No. 2005/0022025) (hereinafter "Application") at paragraph [0017] (emphasis added). Storing the information in clear form is beneficial because the information does not need to be decrypted before it can be read or used either on the client device or by an external device, greatly simplifying rights enforcement and/or usage reporting. This simplification is especially advantageous when a simple, inexpensive client device lacks resources to do unnecessary decryption.

In the Advisory Action, the Examiner argues that *Nonaka* discloses the ability to store rights in an unencrypted (clear text) form, citing *Nonaka* paragraphs [192] and [239]. However, Applicants respectfully submit that, when read in context, paragraphs [192] and [239] clearly teach that rights information is always stored in encrypted form. What *Nonaka* does teach, and what the Examiner mistook for a disclosure that anticipates Claims 1, 20, 31, 34, and 49, is that the rights information need not always be encrypted **by the electronic music distribution ("EMD") service center**, in cases wherein the rights information was previously encrypted **by the content provider**.

By way of background, *Nonaka* discloses a method of distributing encrypted content data from an electronic music distribution center to users. *Nonaka* is a large and complex application that presents some language that is easily misinterpreted. However, having read *Nonaka* completely, Applicants respectfully submit that it does not disclose the ability to store rights in an unencrypted (clear text) form, as claimed in Claims 1, 20, 31, 34, and 49.

For example, one potentially misleading clause in paragraph [192] of *Nonaka* reads as follows: "the UCP [rights] data may not be encrypted **with the license key data** [from the EMD service center]." If one were to read nothing but this clause, then one might believe that *Nonaka* disclosed storing rights in an unencrypted form, as claimed in Claims 1, 20, 31, 34, and 49. However, if one reads that clause in context, one necessarily sees that in the event that the UCP data is not encrypted with the license key data from the EMD service center, "the signature data **encrypted with the private key data of the content provider** is added to the UCP data." Thus, paragraph [192] discloses that rights data is always encrypted, either by the EMD service center or by the content provider.

Similarly, paragraph [239] presents a similar opportunity for a misinterpretation to cause clear error, stating that in some cases, the rights information may be "provided with signature data without being encrypted by the license key data." If one were not familiar with *Nonaka* as a whole, then this clause might again seem to disclose the ability to store rights in an unencrypted form, as claimed in Claims 1, 20, 31, 34, and 49. However, having read *Nonaka* completely, Applicants respectfully submit that although paragraph [239] may disclose that in the event that the rights information is not encrypted "**by the license key data**," the rights information is effectively encrypted by virtue of being "provided with signature data." (Signature data is encrypted rights information. *See Nonaka*, paras [27] ("The public-key encryption circuit… may create the signature data by using the hash values."); [191] ("the signature data [is] encrypted with the private key data… of the EMD service center"); [200] ("the signature data is generated by hashing [(encrypting)] the data used for the signature… by using the private keys…")).

Thus, *Nonaka* teaches that, in all cases, rights information is encrypted or hashed, either by the license key of the EMD service center or by the private key of the content provider, and Applicants respectfully submit that it was clearly improper and without basis to reject Claims 1, 20, 31, 34, and 49 based on the teachings of *Nonaka*.

Notwithstanding the above, it was further clearly improper and without basis to reject Claims 1, 20, 31, 34, and 49 because *Nonaka* does not disclose a "client device key" that is "externally inaccessible from the client device," as claimed in Claims 1, 20, 31, 34, and 49.

Applicants argue that there are two distinct bases on which it can be clearly discerned that *Nonaka* does not disclose the claimed client device key.

First, Applicants respectfully submit that the Application implicitly discloses that the client device key, as claimed in Claims 1, 20, 31, 34, and 49, is unique to each device. For example, "a client device…often includes a hardware key embedded within the device." Application para. [17]. This client key is used, at least in part to track usage and update content usage information and record tampering. *See* Application paras. [39-41]. If the client device key were not unique, but were common to a set of client devices, then it stands to reason that content could be played on many different client devices, at least partially defeating the purpose of controlling content access. *Nonaka*, by contrast, teaches that a "license key" is not tied to a client device, but to a particular piece of content.

Furthermore, neither the Advisory Action nor the Final Office Action were able to refute or even to address Applicant's second argument in any way. This un-refuted argument is that *Nonaka* does not disclose an **externally inaccessible** client device key, as claimed in Claims 1, 20, 31, 34, and 49. On the contrary, *Nonaka* discloses that a "license key" may be sent **across a network** to a client device. *See Nonaka,* paragraphs [99], [304]. Thus, even a cursory reading makes clear that a "license key" as disclosed in *Nonaka* **must be accessible** through an **external** data path (the network). It is equally clear that a "license key" as disclosed in *Nonaka* cannot be externally inaccessible, as is the "client device key" claimed in Claims 1, 20, 31, 34, and 49.

Neither the Final Office Action nor the Advisory Action even addressed this second argument, let alone successfully refuted it. Therefore, it was clearly improper and without basis to say that *Nonaka* discloses a "client device key" that is "externally inaccessible from the client device," as claimed in Claims 1, 20, 31, 34, and 49. All of the remaining claims depend from one of Claims 1, 20, 31, 34, and 49 and are therefore allowable by virtue of such dependency.

CONCLUSION

It was clearly improper and without basis to say that *Nonaka* discloses the ability to store rights in an unencrypted (clear text) form. It was equally clearly improper to say that *Nonaka* discloses a "client device key" that is "externally inaccessible from the client device." Having shown the impropriety of these unsupported rejections, Applicants respectfully submit that independent Claims 1, 20, 31, 34, and 49 and all of their dependencies are in condition for allowance. Accordingly, early and favorable action allowing all of the pending claims and passing this application to issue is respectfully requested. The Examiner is invited to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to Axios Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW GROUP

Date: September 6, 2007 by: /Adam L.K. Philipp/
Adam L.K. Philipp
Direct Dial: 206.217.2226
Reg. No.: 42,071

AXIOS LAW GROUP
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206.217.2200
Customer No.: 61857

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x, OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
1224-2006053

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on September 6, 2007

Signature /Angela M. Martin/

Typed or printed name Angela M. Martin

Application Number	Filed
10/719,674	November 21, 2003

First Named Inventor
Hug, Joshua D.

Art Unit	Examiner
2136	Johnson, Carlton

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☐ attorney or agent of record.
Registration number _____.

☒ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 42,071

/Adam L.K. Philipp/
Signature

Adam L.K. Philipp
Typed or printed name

(206) 217-2200
Telephone number

September 6, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.